Collax Monitoring mit Nagios

Howto

Dieses Howto beschreibt die Konfiguration der Aktiven Überwachung auf einem Collax Server. Intern verwendet das System dafür Nagios. Primär wird Nagios zur Selbstüberwachung des Systems eingesetzt. Es können jedoch auch weitere Systeme im Netzwerk überwacht werden.

Vorraussetzungen

- Collax Business Server
- Collax Security Gateway
- Collax Platform Server

Ziel

In einem Netzwerk sollen bestimmte Dienste der Server und Clients auf Ihre Funktionalität überwacht werden. Beim Ausfall von Diensten wird der Administrator per Email benachrichtigt. Außerdem soll man auf einen Blick erkennen, ob alle Dienste laufen und die Server erreichbar sind.

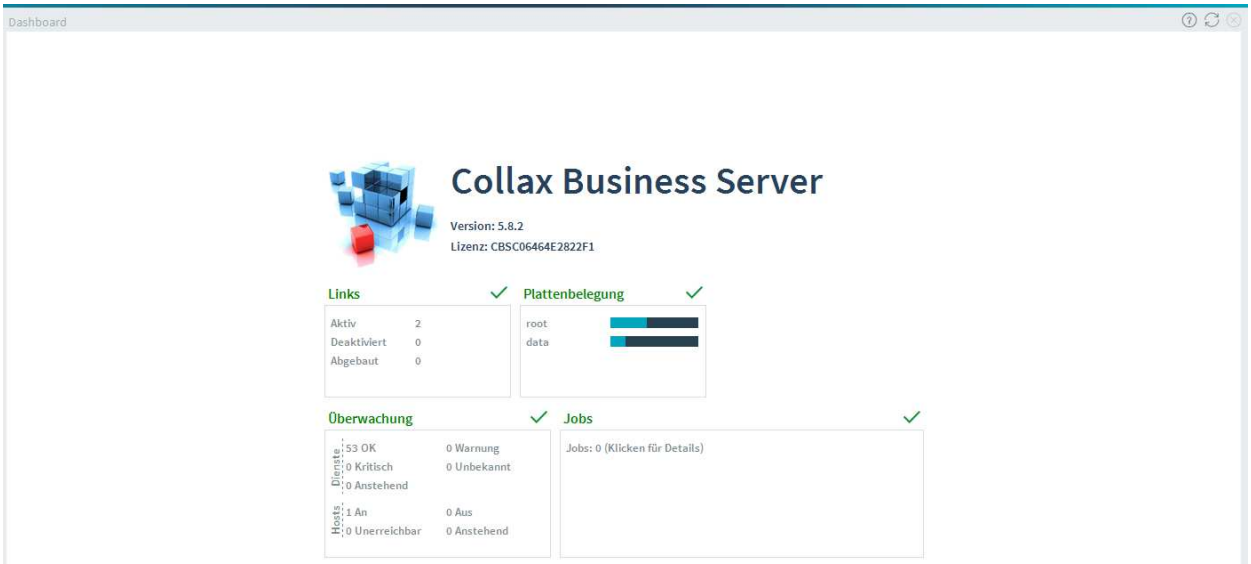
Aufgabe

Der Administrator möchte in seinem Netzwerk einen Client auf dessen Erreichbarkeit überwachen.

Lösung

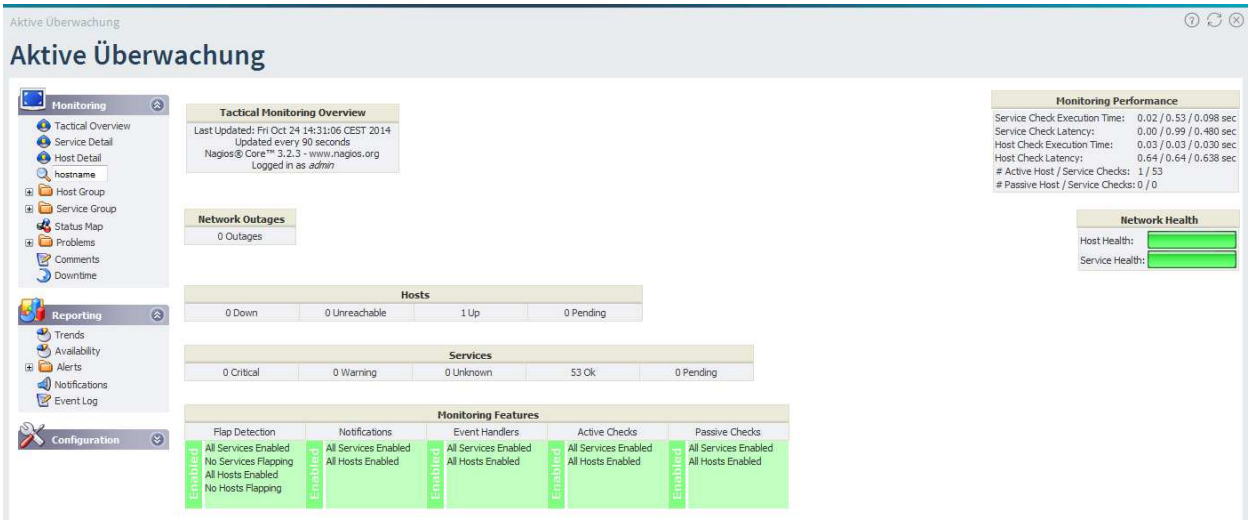
Standardmäßig ist die *Überwachung* auf dem Collax Server bereits aktiviert. Andernfalls erscheint auf dem Dashboard die Meldung „Die aktive Netzwerküberwachung ist nicht aktiviert“ und lässt sich mit einem Klick aktivieren.

Über das Dashboard wird der Gesamtstatus auf einen Blick dargestellt. Der Bereich *Überwachung* gibt auf einen Blick Auskunft, ob die Bereiche Dienste und Hardware ordnungsgemäß funktionieren.



Im Dialog *Überwachung* wird der Status der aktiven Überwachung angezeigt. Intern verwendet das System dazu *Nagios*, dessen Web-GUI hier eingeblendet wird. In dem Menü auf der linken Seite können verschiedene Informationen und Statistiken abgerufen werden.

Wichtig ist das Tactical Overview, welches auf einen Blick den Zustand der überwachten Computer (Hosts) und Dienste (Services) anzeigt. Interessant ist auch die Status Map, in der alle Hosts auf einen Blick erfasst werden können. Zudem visualisiert diese Übersicht die Abhängigkeiten der Systeme untereinander.



Überwachung weiterer Hosts

Collax Server bieten aktive Überwachungstests, mit denen Dienste, Prozesse oder Zustände von anderen Systemen erfasst und ausgewertet werden können. Ein Collax Server agiert in dem beschriebenen Szenario als sogenannter Monitoring-Server. Dieser kann sowohl Windows Systeme als auch Linux-Systeme, insbesondere auch weitere Collax Systeme, mit in die aktive Überwachung aufnehmen.

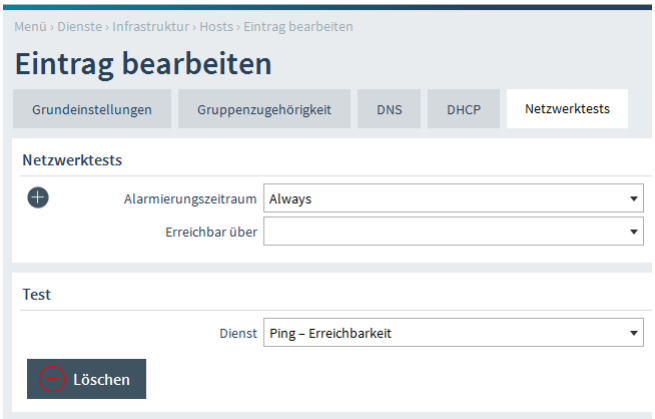
Die Konfiguration weiterer Hosts und der geprüften Dienste auf jedem Host wird in den Einstellungen des jeweiligen Hosts vorgenommen.

Dieser Dialog befindet sich unter *„Dienste → Infrastruktur → DNS → Hosts“*

Über den Reiter *„Netzwerktests“* können für den Host Tests zur Überwachung aktiviert werden.

Über den Button *„Netzwerktest hinzufügen“* können die Dienste angegeben werden, die auf ihre Funktionsfähigkeit hin überwacht werden sollen. Diese Dienste werden dann regelmäßig kontaktiert. Wird ein Dienst als nicht mehr funktionsfähig erkannt, wird ein Alarm ausgelöst.

Hinweis: Die Überwachung funktioniert nur für Rechner, die eine feste IP-Adresse haben.



Alarmierungszeitraum In dieser Liste kann der Zeitraum ausgewählt werden, in dem die unten angegebenen Tests durchgeführt werden und einen Alarm auslösen. Dies ist nützlich, wenn das System nur zu bestimmten Zeiten eingeschaltet ist, etwa während der Bürozeiten.

Erreichbar über Ist das System über ein anderes System, etwa einen Router, erreichbar, kann hier dieser andere Host ausgewählt werden. Bei einem Ausfall des anderen Hosts wird für dieses System keine Überprüfung mehr durchgeführt und kein Alarm ausgelöst. Es wechselt in den Zustand „unbekannt“. Bei Rückkehr des anderen Hosts werden die Tests für dieses System wieder aufgenommen. Nagios nutzt diese Information außerdem zur Darstellung der Netzwerkkarte.

Bleibt das Feld leer, wird versucht, anhand der Routinginformationen den richtigen Router für den Rechner zu finden. Dies funktioniert allerdings nur, wenn der Host lediglich über einen einzigen anderen Router erreicht werden kann.

Wenn jedoch mehrere Router zwischen diesem System und dem Host liegen, sollte hier der letzte bekannte „Hop“ zum gewünschten Host angegeben werden. Wenn der Host „X“ über die Strecke „A“ – „B“ – „C“ erreichbar ist, muss hier „C“ angegeben werden. Für „C“ kann ebenfalls eine Überwachung angelegt werden, „C“ ist dann über „B“ erreichbar.

NRPE

Anhand der Technik von NRPE (Nagios Remote Plugin Executor) können für die Überwachung wichtige Systeminformationen abgerufen werden (z.B.: CPU-, RAM-, Disk-Informationen), welche mit der einfacheren Methode der Protokollüberwachung (z.B.: HTTP, DNS) nicht einsehbar wären.

Überwachung von Windows-Plattformen

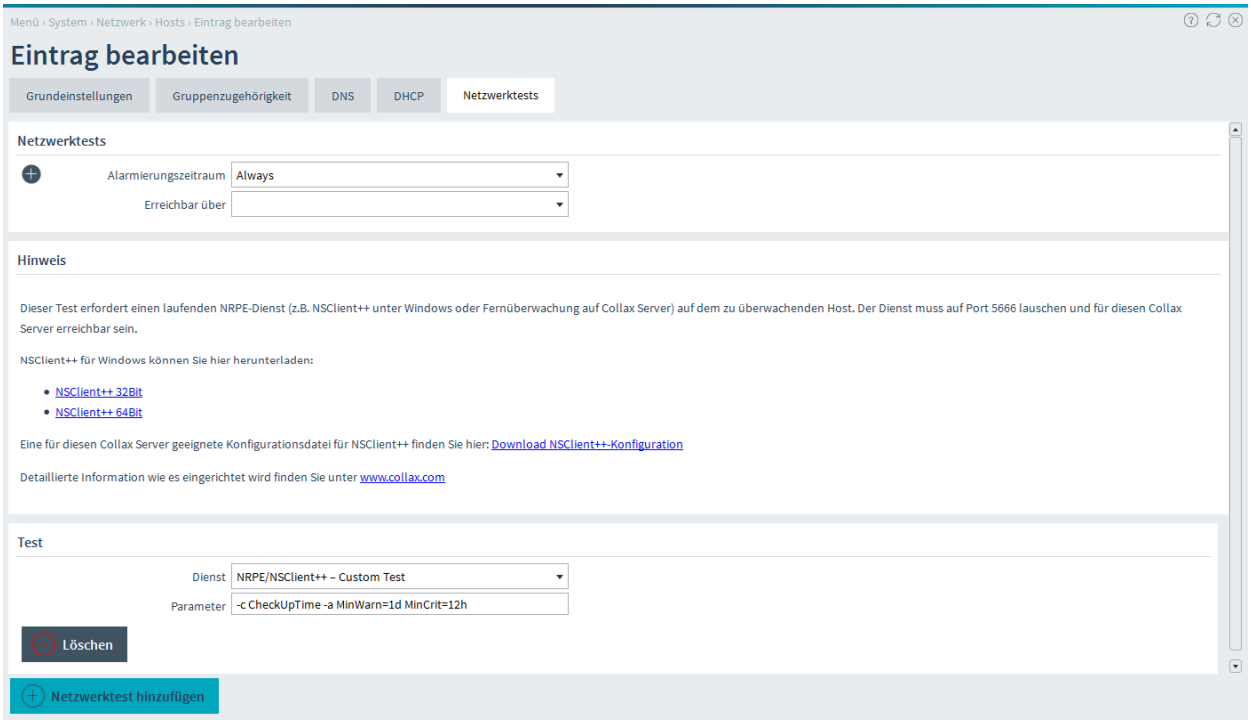
Für die Überwachung von Windows Plattformen durch NRPE wird das Werkzeug NSClient++ benötigt.

Konfiguration des Collax Servers als Monitoring-Server

Für die Überwachung von Windows-Plattformen mittels NRPE werden Überwachungstests in der Administrations-GUI zur Auswahl gestellt. Wählen Sie im Formular Hosts den zu überwachenden Host aus und fügen dann einen Überwachungstest mit überwachtem Dienst *„NRPE/NSClient++ - Custom Test“* hinzu.
Setzen Sie anschließend die gewünschten Parameter, speichern das Formular und aktivieren die Einstellungen.
Am Ende des Howtos finden Sie eine Liste der möglichen Standardtests und deren Parameter. Die aufgeführten Tests dienen als Vorlage und können auf die eigenen Anforderungen angepasst werden.

Installation NSClient++

Die entsprechende Software für 32-Bit- oder 64-Bit-Windows-Systeme kann direkt über das Formular heruntergeladen werden und erscheint bei der Auswahl des Überwachungstests des Dienstes *„NRPE/NSClient++ - Custom Test“*



Um NSClient++ auf dem Zielsystem zu installieren, kann einfach das heruntergeladene MSI-Paket angeklickt und dem Installationsassistenten gefolgt werden. Im Assistenten müssen keine Parameter für die Konfigurationsdatei angegeben werden, denn die Konfiguration wird nach der Installation vorgenommen.

Konfiguration von NSClient++ auf Windows
Bevor NSClient++ gestartet werden kann, muss die INI-Datei der Standardinstallation angepasst werden. Um den NSClient++ sicher betreiben zu können, muss dieser ebenso wissen, welche Monitoring-Server (Parameter allowed_hosts) welche Informationen (Module) abrufen dürfen.

Diese NSC.ini enthält automatisch die Einstellungen für allowed_hosts in Verbindung mit dem NRPE Mechanismus. Um die Vorlage von Collax zu benutzen, kann die heruntergeladene ini-Datei ins Installationsverzeichnis von NSClient++ kopiert werden.
Neben den Allowed_Hosts bietet die Konfiguration schon voreingestellte Module und Tests, die durch einen Collax Server abgefragt werden dürfen.

Starten von NSClient++ auf Windows
Durch die Installation wird NSClient++ als Dienst unter Windows registriert. Deshalb kann nach dem Kopieren der NSC.ini der NSClient++ in der Diensteverwaltung gestartet werden. Für die einwandfreie Abfrage von NSClient++ über das Netzwerk muss der Port 5666 auf dem betreffenden Windows-System in der Firewall geöffnet werden.

Collax stellt hierzu eine, für die Verwendung durch den konfigurierten Collax Server, vorbereitete **NSC.ini** wiederum zum Download im Formular *Überwachungstests* zur Verfügung.

NSClient++ Parameter

Um erste Versuche durchzuführen, kann für einen NRPE/NSClient++-Test eine der nachfolgenden Parameter-Zeilen eins zu eins in die Parameter-Zeile übertragen werden.

Laufwerke

-c CheckDriveSize -a ShowAll MinWarnFree=10% MinCritFree=5% Drive=c:\

Dateigrößen in C:\Windows

-c CheckFileSize -a ShowAll MaxWarn=1024M MaxCrit=4096M File:_WIN=c:\WINDOWS*.*

Dateigröße von pagefile.sys

-c CheckFileSize -a ShowAll MinWarn=512M MinCrit=1G File=c:\pagefile.sys

Mehrere Dateien auf Version prüfen

-c CheckFiles -a path=D:\tmp pattern=*.exe "filter=version != 1.0" "syntax=%filename%: %version%" warn=gt:1 crit==1

Mehrere Dateien auf Größe prüfen

-c CheckFiles -a path=D:\tmp pattern=*.txt "filter=size gt 20" "syntax=%filename%: %size%" MaxWarn=1

Eventlog ID prüfen

-c CheckEventLog -a filter=new file=Application filter+eventID==18456 filter-generated=1h MaxWarn=5 MaxCrit=10 descriptions unique

CPU-Auslastung < 80%

-c CheckCPU -a warn=80 crit=90 time=20m time=10s time=4

CPU-Auslastung wie in Linux

-c CheckCPU -a warn=100 crit=100 time=1 warn=95 crit=99 time=5 warn=90 crit=95 time=15

Uptime testen

-c CheckUpTime -a MinWarn=1d MinCrit=12h

Alle automatisch zu startenden Dienste testen, außer wampmysqld und MpfService

-c CheckServiceState -a CheckAll exclude=wampmysqld exclude=MpfService

Prozesse NSCLient++ und cmd.exe prüfen System-Monitoring mit Collax und NRPE

-c CheckProcState -a ShowAll cmd.exe=stopped NSClient++.exe=started

Speicherauslastung < 80%

-c CheckMEM -a MaxWarn=80% MaxCrit=90% ShowAll type=physical

Für weitere Anwendungsfälle der Checks können diese Detailseiten aufgerufen werden. Sie enthalten genaue Spezifikationen und Beschreibungen der einzelnen Checks. Für *CheckWMI* und *CheckEventLog* sind zusätzlich Kenntnisse über Windows Management Instrumentation und über Windows Eventlogs erforderlich.

CheckWMI http://www.nsclient.org/nscp/wiki/CheckWMI
CheckFileSize http://www.nsclient.org/nscp/wiki/CheckFileSize
CheckDriveSize http://www.nsclient.org/nscp/wiki/CheckDriveSize
CheckFiles http://www.nsclient.org/nscp/wiki/CheckFiles
CheckEventLog http://www.nsclient.org/nscp/wiki/CheckEventLog
CheckCPU http://www.nsclient.org/nscp/wiki/CheckCPU
CheckUpTime http://www.nsclient.org/nscp/wiki/CheckUpTime
CheckServiceState http://www.nsclient.org/nscp/wiki/CheckServiceState
CheckProcState http://www.nsclient.org/nscp/wiki/CheckProcState
CheckMem http://www.nsclient.org/nscp/wiki/